CLAIMS

What is claimed is:

1. An authentication method wherein:

a user owns an electronic value including encrypted value authentication information (F(VPW)) wherein said authentication information (VPW) corresponding to said electronic value specified by user is encoded by a first irreversible calculation process (F),

in process for authenticating user as the right owner of said electronic value, authentication side generates a random number (R) and transmits it to user side,

a user side generates value authentication information (F(VPW')) from authentication information (VPW) corresponding to an electronic value input by user, further generates authentication information (G(R,F(VPW'))) wherein said random number (R) and value authentication information (F(VPW')) are concatenated and encoded by a second irreversible calculation process (G) and transmits said electronic value and authentication information (G(R,F(VPW'))) to said authentication side,

said authentication side decrypts code of received electronic value, extracts value authentication information (F(VPW)) from electronic value, generates authentication information (G(R,F(VPW))) wherein said random number (R) and value authentication information (F(VPW)) are concatenated and encoded by said second irreversible calculation process (G), collates said received authentication information (G(R,F(VPW'))) with said generated authentication information (G(R,F(VPW))), verifies that they are identical, and authenticates user.

2. The authentication method of claim 1 wherein:

a decryption key of encrypted part of said electronic value is generated from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by a third irreversible calculation process (H) and master key,

in process for authenticating user as the rightful owner of said electronic value, said user side further generates data (H(F(VPW'))) wherein value authentication

information (F(VPW')) is encoded by said third irreversible calculation process (H), transmits data (H(F(VPW'))) with said electronic value and said authentication information (G(R,F(VPW'))) to said authentication side,

said authentication side generates a decryption key from received data (H(F(VPW'))) and master key, and decrypts code of received electronic value.

3. A mutual authentication method wherein:

a user owns an electronic value including an encrypted value authentication information (F(VPW)) wherein authentication information (VPW) corresponding to said electronic value specified by user is encoded by a first irreversible calculation process (F),

in a mutual authentication process, wherein a user is authenticated as the rightful owner of said electronic value and user authenticates the authentication side, authentication side generates a first random number (R1) and transmits it to user side,

said user side generates value authentication information (F(VPW')) from authentication information (VPW') corresponding to electronic value input by user, generates a second random number (R2), further generates authentication information (G(R1,F(VPW'))) wherein said first random number (R1) and said value authentication information (F(VPW')) are concatenated and encoded by a second irreversible calculation process (G) and transmits said electronic value, authentication information (G(R1,F(VPW'))) and second random number (R2) to said authentication side,

authentication side decrypts code of received electronic value, extracts value authentication information (F(VPW)) from said electronic value, generates authentication information (G(R1,F(VPW))) wherein said first random number (R1) and value authentication information (F(VPW)) are concatenated and encoded by a second irreversible calculation process (G), collates said received authentication information (G(R1,F(VPW'))) with said generated authentication information (G(R1,F(VPW))), verifies that they are identical, and authenticates user,

further generates authentication information (I(R1,R2,F(VPW))) wherein said

first random number (R1), said second random number (R2) and value authentication information (F(VPW)) are concatenated and encoded by a fourth irreversible calculation process (I), transmits it to user side,

said user side generates authentication information (I(R1,R2,F(VPW'))) wherein said first random number (R1), said second random number (R2) and value authentication information (F(VPW')) are concatenated and encoded by said fourth irreversible calculation process (I), collates said received authentication information (I(R1,R2,F(VPW))) with said generated authentication information (I(R1,R2,F(VPW'))), verifies that they are identical, and authenticates authentication side.

4. The mutual authentication method of claim 3 wherein:

said decryption key of encrypted part of said electronic value is generated from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by said second irreversible calculation process (H) and master key,

in mutual authentication process wherein authentication side authenticates user as the rightful owner of said electronic value and user authenticates the authentication side, said user side further generates data (H(F(VPW'))) wherein value authentication information (F(VPW')) is encoded by said third irreversible calculation process (H), transmits data (H(F(VPW'))), said electronic value, said authentication information (G(R1,F(VPW'))), and said second random number (R2) to authentication side

authentication side generates said decryption key from received data (H(F(VPW'))) and master key, and decrypts code of said received electronic value.

5. An update processing method wherein:

a user owns electronic value including an encrypted value authentication information (F(VPW)) wherein authentication information (VPW) corresponding to electronic value specified by user is encoded by a first irreversible calculation process (F),

in update process wherein authentication side validates said electronic value

and updates content of electronic value, authentication side generates a first random number (R1) and transmits it to user side,

user side generates value authentication information (F(VPW')) from authentication information (VPW') corresponding to electronic value input by user, generates a second random number (R2), further generates authentication information (G(R1,F(VPW'))) wherein said first random number (R1) and said value authentication information (F(VPW')) are concatenated and encoded by a second irreversible calculation process (G) and transmits said electronic value, authentication information (G(R1,F(VPW'))) and said second random number (R2) to authentication side,

authentication side decrypts code of received said electronic value, extracts value authentication information (F(VPW)) from said electronic value, generates value authentication information (G(R1,F(VPW))) wherein said first random number (R1) and value authentication information (F(VPW)) are concatenated and encoded by said second irreversible calculation process (G), collates said received authentication information (G(R1,F(VPW'))) with said generated authentication information (G(R1,F(VPW))), verifies that they are identical, and authenticates user,

further generates said electronic value whose content is updated, further generates authentication information (I(R1,R2,F(VPW))) wherein said first random number (R1), said second random number (R2) and value authentication information (F(VPW)) are concatenated and encoded by a third irreversible calculation process (I), transmits said electronic value whose content is updated to user side and authentication information (I(R1,R2,F(VPW))) to user side,

user side generates authentication information (I(R1,R2,F(VPW'))) wherein said first random number (R1), said second random number (R2) and value authentication information (F(VPW')) are concatenated and encoded by said third irreversible calculation process (I), collates said received authentication information (I(R1,R2,F(VPW))) with generated authentication information (I(R1,R2,F(VPW'))), verifies that they are identical, authenticates authentication side, and updates

electronic value to received said electronic value whose content is updated.

6. The update processing method of claim 5 wherein:

a decryption key of encrypted part of said electronic value is generated from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by said third irreversible calculation process (H) and master key,

in update process wherein authentication side validates said electronic value and updates content of electronic value, user side further generates data (H(F(VPW'))) wherein value authentication information (F(VPW')) is encoded by said third irreversible calculation process (H), transmits data (H(F(VPW'))), said electronic value, said authentication information (G(R1,F(VPW'))), and said second random number (R2) to authentication side

authentication side generates said decryption key from received data (H(F(VPW'))), and a master key decrypts code of received electronic value.

7. A mobile terminal wherein:

comprising storage means storing electronic value, generating value authentication information (F(VPW')) wherein value authentication information (VPW) corresponding to said electronic value input by a user is encoded by a first irreversible calculation process (F), further generating a second random number (R2), further encoding by an irreversible calculation process (F) on data wherein said value authentication information (F(VPW')) and a first random number (R1) received from authentication apparatus are concatenated, generating authentication information (G(R1,F(VPW'))), and transmitting said electronic value, authentication information (G(R1,F(VPW'))) and said second random number (R2) to authentication apparatus, thereby authenticating user to be the rightful owner of said electronic value.

8. A mobile terminal wherein:

comprising storage means storing electronic value, generating value authentication information (F(VPW')) wherein value authentication information (VPW) corresponding to said electronic value input by a user is encoded by a first irreversible

calculation process (F), further generating a second random number (R2), further encoded by a second irreversible calculation process (G) on data wherein said value authentication information (F(VPW')) and a first random number (R1) received from authentication apparatus are concatenated, generating authentication information (G(R1,F(VPW'))), and transmitting said electronic value, authentication information (G(R1,F(VPW'))) and said second random number (R2) to authentication apparatus, thereby authenticating user to be the rightful owner of said electronic value, generating authentication information (I(R1,R2,F(VPW'))) wherein said first random number (R1), said second random number (R2) and value authentication information (F(VPW')) are concatenated and encoded by a third irreversible calculation process (I), collating said authentication information (I(R1,R2,F(VPW))) received from said authentication apparatus with generated authentication information (I(R1,R2,F(VPW'))), verifying that they are identical, and authenticating said authentication apparatus.

9. A mobile terminal wherein:

comprising storage means storing an electronic value, generating value authentication information (F(VPW')) wherein value authentication information (VPW) corresponding to said electronic value input by a user is encoded by a first irreversible calculation process (F), further generating a first random number (R2), further encoding by a second irreversible calculation process (G) on data wherein said value authentication information (F(VPW')) and said first random number (R1) received from authentication apparatus are concatenated, generating authentication information (G(R1,F(VPW'))), and transmitting said electronic value, authentication information (G(R1,F(VPW'))) and said second random number (R2) to authentication apparatus, thereby authenticating user to be the rightful owner of said electronic value, generating authentication information (I(R1,R2,F(VPW'))) wherein said first random number (R1), said second random number (R2) and value authentication information (F(VPW')) are concatenated and encoded by a third irreversible calculation process (I), collating said authentication information (I(R1,R2,F(VPW))) received from said authentication

apparatus with generated authentication information (I(R1,R2,F(VPW'))), verifying that they are identical, and authenticating said authentication apparatus, and updating said electronic value to electronic value received from said authentication apparatus.

10. The mobile terminal of any one of claims 7 to 9 wherein:

decryption key of encrypted part of said electronic value is generated from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by a fourth irreversible calculation process (H) and master key, said mobile terminal generates data (H(F(VPW'))) wherein value authentication information (F(VPW')) is encoded by said fourth irreversible calculation process (H) and transmits said electronic value, said authentication information (G(R,F(VPW'))) and data (H(F(VPW)))to authentication apparatus, thereby authenticating user to be the rightful owner of said electronic value.

11. The mobile terminal of any one of claims 7 to 9 wherein:

said storage means stores a property which is attribute information set with respect to each electronic value with said electronic value,

in authentication process with the use of said electronic value, an operation is executed based on said property.

12. The mobile terminal of any one of claims 7 to 9 wherein:

said storage means stores property which is attribute information set with respect to each electronic value with said electronic value,

in authentication process with the use of said electronic value, an operation is executed based on user terminal control information received from said authentication information and said property.

13. An authentication apparatus wherein:

generating a random number (R) and transmitting it to mobile terminal, receiving authentication information (G(R,F(VPW'))) and electronic value from said mobile terminal, decrypting code of encrypted part of electronic value, and validating said electronic value, further extracting value authentication information (F(VPW))

from said electronic value, generating authentication information (G(R,F(VPW))) wherein value authentication information (F(VPW)) and random number (R) are concatenated and encoded by an irreversible calculation process (G), and collating received authentication information (G(R,F(VPW'))) with generated authentication information (G(R,F(VPW))), verifying that they are identical, thereby authenticating user.

14. An authentication apparatus wherein:

generating a first random number (R1) and transmitting it to mobile terminal, receiving authentication information (G(R1,F(VPW'))), electronic value and a second random number (R2) from said mobile terminal, decrypting code of encrypted part of electronic value, and validating said electronic value, further extracting value authentication information (F(VPW)), generating authentication information (G(R1,F(VPW))) wherein value authentication information (F(VPW)) and said first random number (R1) are concatenated and encoded by a irreversible calculation process (G), and collating received authentication information (G(R1,F(VPW'))) with generated authentication information (G(R1,F(VPW))), verifying that they are identical, authenticating user, further generating authentication information (I(R1,R2,F(VPW))) wherein value authentication information (F(VPW)), said first random number (R1) and said second random number (R2) received from mobile terminal are concatenated and encoded by a irreversible calculation process (I), and transmitting said authentication information (I(R1,R2,F(VPW))) to user side, thereby being authenticated by mobile terminal.

15. An authentication apparatus wherein:

generating a first random number (R1) and transmitting it to mobile terminal, receiving authentication information (G(R1,F(VPW'))), electronic value and a second random number (R2) from said mobile terminal, decrypting code of encrypted part of electronic value, and validating said electronic value, further extracting value authentication information (F(VPW)), generating authentication information

(G(R1,F(VPW))) wherein value authentication information (F(VPW)) and said first random number (R1) are concatenated and encoded by a first irreversible calculation process (G), and collating received authentication information (G(R1,F(VPW'))) with generated authentication information (G(R1,F(VPW))), verifying that they are identical, authenticating user, further generates electronic value whose content is updated, further generates authentication information (I(R1,R2,F(VPW))) wherein value authentication information (F(VPW)), said first random number (R1) and said second random number (R2) received from mobile terminal are concatenated and encoded by a second irreversible calculation process (I), and transmitting said authentication information (I(R1,R2,F(VPW))) to user side, and updating electronic value in mobile terminal to said updated electronic value.

16. The authentication apparatus of any one of claims 13 to 15 wherein:

a decryption key of encrypted part of said electronic value is generated from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by a third irreversible calculation process (H) and master key,

said authentication apparatus generates said decryption key from data (H(F(VPW'))) received from said mobile terminal and master key, and decrypts code of received electronic value.

17. The authentication apparatus of any one of claims 13 to 15, comprising a security module having a tamper-resistant function, wherein:

said security module decrypts the encrypted part of said electronic value, stores a negative list of electronic values, and verifies that said received electronic value is not listed in said negative list of electronic value at the point of validation of said received electronic value.

18. The authentication apparatus of claim 17 wherein:

said security module communicates with a center and updates information stored in said security module.

19. The authentication apparatus of any one of claims 13 to 15 wherein:

transmitting user terminal information to a mobile terminal and controlling operation of said mobile terminal at the point of authentication process by said electronic value and executing operation of its own based on service terminal control information received from said mobile terminal.

20. An electronic value issuance server wherein:

extracting authentication information (VPW) corresponding to an electronic value specified by user from electronic value issuance request received from said mobile terminal, generating value authentication information (F(VPW)) wherein authentication information (VPW) corresponding to said electronic value is encoded by said first irreversible calculation process (F), generating encryption key from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by a third irreversible calculation process (H) and master key, generating said electronic value with the use of said value authentication information (F(VPW)) and said generated encryption key, and transmitting it to said mobile terminal.

21. An electronic value issuance server wherein:

extracting authentication information (F(VPW)) corresponding to an electronic value specified by user, wherein authentication information (VPW) is encoded by a first irreversible calculation process (F), from electronic value issuance request message received from a mobile terminal, generating encryption key from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by a second irreversible calculation process (H) and a master key, generating said electronic value with the use of said value authentication information (F(VPW)) and said generated encryption key, and transmitting it to mobile terminal.

22. The electronic value issuance server of either claim 20 or 21 wherein:

said electronic value includes electronic value public information and security information,

said security information is data wherein electronic value secret information, said value authentication information (F(VPW)) and signature information are

encrypted by said generated encryption key,

said signature information is a digital signature for data wherein said electronic value public information, said electronic value secret information, and said value authentication information (F(VPW)) are concatenated.

23. The electronic value issuance server of either claim 20 or 21 wherein:

said electronic value includes electronic value public information and security information,

said security information is data wherein electronic value secret information, said value authentication information (F(VPW)) and signature information are encrypted by said generated encryption key,

said signature information is a result of a hash calculation for data wherein said electronic value public information, said electronic value secret information, and said value authentication information (F(VPW)) are concatenated.

24. The electronic value issuance server of claim 22 wherein:

generating risk management information based on credit information of a user and result of risk evaluation on authentication information (F(VPW)) corresponding to said electronic value specified by user and building said risk management information in said electronic value secret information.

25. An authentication system, comprised of mobile terminal managed by user, authentication apparatus and electronic value issuance server, wherein:

said mobile terminal stores electronic value received from said electronic value issuance server,

said electronic value includes an encrypted value authentication information (F(VPW)) wherein authentication information (VPW) corresponding to electronic value specified by user is encoded by a first irreversible calculation process (F),

in process for authenticating user to be the rightful owner of said electronic value, authentication apparatus generates random number (R) and transmits it to mobile terminal,

mobile terminal generates value authentication information (F(VPW')) from authentication information (VPW') corresponding to electronic value specified by user, further generates authentication information (G(R,F(VPW'))) wherein value authentication information (F(VPW')) and said random number (R) are concatenated and encoded by a second irreversible calculation process (G), and transmits said electronic value and authentication information (G(R,F(VPW'))) to said authentication apparatus,

authentication apparatus decrypts code of received electronic value, extracts value authentication information (F(VPW)) from electronic value, generates authentication information (G(R,F(VPW))) wherein value authentication information (F(VPW)) and said random number (R) are concatenated and encoded by said second irreversible calculation process (G), collates said received authentication information (G(R,F(VPW'))) with said generated authentication information (G(R,F(VPW))), verifies that they are identical, and authenticates user.

26. The authentication system of claim 25 wherein:

said decryption key of encrypted part of said electronic value is generated from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by a third irreversible calculation process (H) and master key,

in process for authenticating user as the right owner of said electronic value, said user side further generates data (H(F(VPW'))) wherein value authentication information (F(VPW')) is encoded by a third irreversible calculation process (H), transmits data (H(F(VPW'))) with said electronic value and said authentication information (G(R,F(VPW'))) to authentication apparatus,

authentication apparatus generates decryption key from received data (H(F(VPW'))) and master key, decrypts code of received electronic value.

27. A mutual authentication system, comprised of mobile terminal managed by user, authentication apparatus and electronic value issuance server, wherein:

said mobile terminal stores electronic value received from said electronic value

issuance server,

said electronic value includes an encrypted value authentication information (F(VPW)) wherein authentication information (VPW) corresponding to electronic value specified by user is encoded by a first irreversible calculation process (F),

in mutual authentication process wherein authentication apparatus authenticates user as the right owner of said electronic value and user authenticates authentication apparatus,

authentication apparatus generates a first random number (R1) and transmits it to mobile terminal

mobile terminal generates value authentication information (F(VPW')) from authentication information (VPW') corresponding to electronic value specified by user, further generates a second random number (R2), further generates authentication information (G(R1,F(VPW'))) wherein value authentication information (F(VPW')) and said first random number (R1) are concatenated and encoded by a second irreversible calculation process (G), transmits said electronic value, authentication information (G(R1,F(VPW'))) and said second random number (R2) to said authentication apparatus,

authentication apparatus decrypts code of received electronic value, extracts value authentication information (F(VPW)) from electronic value, generates authentication information (G(R1,F(VPW))) wherein value authentication information (F(VPW)) and said first random number (R1) are concatenated and encoded by said second irreversible calculation process (G), collates said received authentication information (G(R1,F(VPW'))) with said generated authentication information (G(R1,F(VPW))), verifies that they are identical, and authenticates user, further generates authentication information (I(R1,R2,F(VPW))) wherein value authentication information (F(VPW)), said first random number (R1), and said second random number (R2) are concatenated and encoded by a third irreversible calculation process (I), and transmits it to mobile terminal,

mobile terminal generates authentication information (I(R1,R2,F(VPW'))) wherein value authentication information (F(VPW')), said first random number (R1), and said second random number (R2) are concatenated and encoded by said third irreversible calculation process (I), collates said received authentication information (G(R1,F(VPW))) with said generated authentication information (G(R1,F(VPW'))), verifies that they are identical, and authenticates authentication apparatus.

28. The mutual authentication system of claim 27 wherein:

decryption key of encrypted part of said electronic value is generated from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by a fourth irreversible calculation process (H) and a master key,

in mutual authentication process wherein authentication apparatus authenticates user as the rightful owner of said electronic value and user authenticates the authentication apparatus, mobile terminal further generates data (H(F(VPW'))) wherein value authentication information (F(VPW')) is encoded by said fourth irreversible calculation process (H), transmits data (H(F(VPW'))), said electronic value, said authentication information (G(R1,F(VPW'))), and said second random number (R2) to authentication apparatus,

said authentication apparatus generates a decryption key from received data (H(F(VPW'))) and said master key, decrypts code of received electronic value.

29. An electronic value update system wherein:

a mobile terminal stores an electronic value received from an electronic value issuance server,

said electronic value includes encrypted value authentication information (F(VPW)) wherein authentication information (VPW) corresponding to electronic value specified by user is encoded by a first irreversible calculation process (F),

an authentication apparatus validates said electronic value and updates content of electronic value during updated,

said authentication apparatus generates a first random number (R1) and

transmits it to said mobile terminal

said mobile terminal generates value authentication information (F(VPW')) from authentication information (VPW') corresponding to an electronic value specified by a user, further generates a second random number (R2), further generates authentication information (G(R,F(VPW'))) wherein value authentication information (F(VPW')) and said first random number (R1) are concatenated and encoded by a second irreversible calculation process (G), and transmits said electronic value, authentication information (G(R1,F(VPW'))) and said second random number (R2) to said authentication apparatus,

authentication apparatus decrypts code of said received electronic value, extracts value authentication information (F(VPW)) from said electronic value, generates authentication information (G(R1,F(VPW))) wherein value authentication information (F(VPW)) and said first random number (R1) are concatenated and encoded by said second irreversible calculation process (G), collates said received authentication information (G(R1,F(VPW'))) with said generated authentication information (G(R1,F(VPW))), verifies that they are identical, and authenticates the user, further generates authentication information (I(R1,R2,F(VPW))) wherein value authentication information (F(VPW)), said first random number (R1), and said second random number (R2) are concatenated and encoded by a third irreversible calculation process (I), transmits said electronic value whose content is updated and authentication information (I(R1,R2,F(VPW))) to said mobile terminal,

said mobile terminal generates authentication information (I(R1,R2,F(VPW'))) wherein value authentication information (F(VPW')), said first random number (R1), and said second random number (R2) are concatenated and encoded by said third irreversible calculation process (I), collates said received authentication information (G(R1,F(VPW))) with said generated authentication information (G(R1,F(VPW'))), verifies that they are identical, and authenticates authentication apparatus, and updates said electronic value to said received electronic value.

30. The electronic value update system of claim 29 wherein:

a decryption key of encrypted part of said electronic value is generated from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by a fourth irreversible calculation process (H) and master key,

in update process wherein authentication apparatus validates said electronic value and updates content of electronic value, mobile terminal further generates data (H(F(VPW'))) wherein value authentication information (F(VPW')) is encoded by said fourth irreversible calculation process (H), transmits data (H(F(VPW'))), said electronic value, said authentication information (G(R1,F(VPW'))), and said second random number (R2) to said authentication apparatus,

said authentication apparatus generates said decryption key from received data (H(F(VPW'))) and master key, decrypts code of received electronic value.

31. A lock apparatus wherein:

in issuance of electronic key, an issuance function of electronic key extracting authentication information (F(VPW)) corresponding to electronic key specified by a user, wherein authentication information (VPW) is encoded by a first irreversible calculation process (F), from an electronic key issuance request message received from a mobile terminal, generating an encryption key from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by a second irreversible calculation process (H) and a master key, generating electronic key with the use of said value authentication information (F(VPW)) and said generated encryption key, and transmits it to said mobile terminal,

in authentication of electronic key, an authentication function of electronic key generating a random number (R) and transmitting it to said mobile terminal, receiving authentication information (G(R,F(VPW'))) and said electronic key from said mobile terminal, decrypting code of encrypted part of said electronic key, and validating said electronic key, further extracting value authentication information (F(VPW)) from said electronic key, generating authentication information (G(R,F(VPW))) wherein value

authentication information (F(VPW)) and said random number (R) are concatenated and encoded by a third irreversible calculation process (G), and collating received authentication information (G(R,F(VPW'))) with generated authentication information (G(R,F(VPW))), verifying that they are identical, thereby authenticating user.

32. The lock apparatus of claim 31 wherein:

in issuance of electronic key, generating a second random number (R0), transmitting it to mobile terminal, extracting user identification information (J(LN',R0)) wherein lock number (LN') input to mobile phone by user and said second random number (R0) are concatenated and encoded by a fourth irreversible calculation process (J) from electronic key issuance request message received from mobile terminal, generating user identification information (J(LN,R0)) wherein lock number (LN) and said second random number (R0) are concatenated and encoded by a fourth irreversible calculation process (J), collating received user identification information (J(LN',R0)) with generated user identification information (J(LN,R0)), verifying that they are identical, and authenticating user, thereby issuing an electronic key.

33. The lock apparatus of claim 31 or 32 wherein:

having storage means storing key ID of said issued electronic key,

in authentication of electronic key, collating received key ID of electronic key with key ID stored in said storage means,

executing authentication process based on said authentication information (G(R,F(VPW'))) received from said mobile terminal and said electronic key.

34. An authentication request apparatus, requesting authentication to authentication apparatus, comprising an encrypted first information acquisition unit acquiring encrypted first information wherein the first information is encrypted in a form that can be decrypted by a decryption key stored in said authentication apparatus,

a second information acquisition unit acquiring the second information, is to determine whether the relationship with said first information is a predetermined relationship,

a transmission unit transmitting encrypted first information acquired by said encrypted first information acquisition unit in relation to the second information acquired by said second information acquisition unit to said authentication apparatus.

35. The authentication request apparatus of claim 34, comprising encrypted first information storage unit, wherein said encrypted first information acquisition unit acquires encrypted first information stored in an encrypted first information storage unit.

36. The authentication request apparatus of claim 34 or 35, comprising authentication information input unit for inputting authentication information, the purpose of which is to authenticate, and authentication information processing unit processing authentication information input by said authentication information input unit,

wherein said the second information is information processed by authentication information processing unit.

37. The authentication request apparatus of claim 36 wherein said authentication information processing unit processes said authentication information by a hash calculation.

38. An authentication apparatus comprising a reception unit receiving encrypted first information transmitted from a transmission unit of an authentication request apparatus and the second information transmitted in relation to the encrypted first information, a decryption key storage unit stores decryption key for decrypting encrypted first information, a decryption unit decrypting encrypted first information received by reception unit with the use of said decryption key stored in said decryption key storage unit and acquiring the first information, and a determination unit determining whether the first information decrypted by decryption unit and the second information received in relation to encrypted first information, which is the first information before being decrypted, have a predetermined relationship.

39. An information relating apparatus comprising an authentication

information acquisition unit acquiring authentication information, the first information generation unit generating the first information having a predetermined relationship with said authentication information with the use of authentication information acquired by authentication information acquisition unit, an encryption key storage unit storing encryption key, and an encryption unit encrypting the first information generated by said first information generation unit with the use of encryption key stored by said encryption key storage unit.